⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2-249333

⑤1Int. Cl.[5]　識別記号　庁内整理番号　⑬公開　平成2年(1990)10月5日

H 04 L 9/06
9/14

6945-5K　H 04 L 9/02　Z

審査請求　未請求　請求項の数 1　(全5頁)

⑭発明の名称　秘話装置

⑳特　願　平1-70200

㉒出　願　平1(1989)3月22日

㉑発明者　平出　順二　大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内

㉑発明者　多田　順次　大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内

㉑出願人　シャープ株式会社　大阪府大阪市阿倍野区長池町22番22号

㉔代理人　弁理士　山口　邦夫

明　細　書

1．発明の名称

秘　話　装　置

2．特許請求の範囲

(1)送信側は、

切り替え可能な帰還路を有するシフト・レジスタを用いた第1疑似ランダム信号発生回路と、

暗号鍵を設定する暗号鍵設定手段と、

上記疑似ランダム信号発生回路の初期値及び帰還路設定データを記憶した第1記憶回路と、

上記暗号鍵に応じて上記第1記憶回路から上記初期値及び帰還路設定データを読出し、上記第1疑似ランダム信号発生回路を設定する第1制御手段と、

上記暗号鍵に応じたパラレル・アドレス信号をシリアル・アドレス信号に変換する第1変換回路と、

上記第1疑似ランダム信号発生回路の出力信号により入力データを暗号化する暗号化回路とを具え、

該暗号化回路の出力データ及び上記シリアル・アドレス信号を送信し、

受信側は、

上記第1疑似ランダム信号発生回路と同じ構成の第2疑似ランダム信号発生回路と、

上記第1記憶回路と同じ内容を記憶した第2記憶回路と、

受信した上記シリアル・アドレス信号をパラレル・アドレス信号に変換する第2変換回路と、

該第2変換回路からのパラレル・アドレス信号により、上記第2記憶回路から上記初期値及び帰還路設定データを読出し、上記第2疑似ランダム信号発生回路を設定する第2制御手段と、

上記第2疑似ランダム信号発生回路の出力信号により、受信したデータを復号化する復号化回路とを具えたことを特徴とする秘話装置。

2．発明の詳細な説明

【産業上の利用分野】

本発明は、有線及び無線デジタル通信における秘話装置に関する。

［従来の技術］

有線及び無線通信において、通信内容が秘密の場合、秘話通信を行なう必要がある。そのために、送信側では、通常のデータ（平文）を暗号化して、有線又は無線の通信区間を暗号データ（暗号文）で通信する。そして、受信側にて、この暗号文を変換文に復号化する。

第４図は、従来の秘話装置を示す。送信側においては、暗号化回路１３が、暗号化鍵（暗号化を制御する手段）１５に応じて平文を暗号文に変換する。

暗号化回路１３からの暗号文は、有線又は無線の通信区間を介して、受信側に供給される。

受信側では、復号化回路１４が、復号化鍵（復号化を制御する手段）１６に応じて、暗号文を平文に変換する。

［発明が解決しようとする課題］

第４図に示した従来の秘話装置では、送信側及び受信側が、暗号化及び復号化のために、同一又は独立した鍵を所有する必要がある。これら鍵は、暗号に応じて予め定めておく必要があり、暗号を変更する際は、その度毎に、新たに鍵を取り決める必要がある。

よって、暗号の鍵を設定したり、変更するのが非常に煩わしかった。しかし、通信の秘密を確保するには、度々、暗号の鍵を変更する必要があった。

したがって、本発明の目的は、暗号を変更する際に、鍵を変更する必要がなく、暗号の設定及び変更が容易に行える秘話装置の提供にある。

［課題を解決するための手段］

本発明の秘話装置は、送信側と受信側とに別れている。

送信側は、切り替え可能な帰還路を有するシフト・レジスタを用いた第１疑似ランダム信号発生回路と、

暗号鍵を設定する暗号鍵設定手段と、

疑似ランダム信号発生回路の初期値及び帰還路設定データを記憶した第１記憶回路と、

暗号鍵に応じて第１記憶回路から初期値及び帰還路設定データを読出し、第１疑似ランダム信号発生回路を設定する第１制御手段と、

暗号鍵に応じたパラレル・アドレス信号をシリアル・アドレス信号に変換する第１変換回路と、

第１疑似ランダム信号発生回路の出力信号により入力データを暗号化する暗号化回路とを具えている。

そして、送信側は、暗号化回路の出力データ及びシリアル・アドレス信号を送信する。

また、受信側は、第１疑似ランダム信号発生回路と同じ構成の第２疑似ランダム信号発生回路と、

第１記憶回路と同じ内容を記憶した第２記憶回路と、

受信したシリアル・アドレス信号をパラレル・アドレス信号に変換する第２変換回路と、

この第２変換回路からのパラレル・アドレス信号により、第２記憶回路から初期値及び帰還路設定データを読出し、第２疑似ランダム信号発生回路を設定する第２制御手段と、

第２疑似ランダム信号発生回路の出力信号により、受信したデータを復号化する復号化回路とを具えている。

［作　用］

送信側及び受信側の第１及び第２疑似ランダム信号発生回路は、切り替え可能な帰還路を有するシフト・レジスタを用いている。よって、帰還路及び初期値を変更することにより、種々の異なる疑似ランダム信号を発生できる。

一方、第１及び第２記憶回路は、疑似ランダム信号発生回路の初期値及び帰還路設定データの複数組を記憶している。よって、暗号鍵設定手段の設定に応じて、記憶回路の記憶内容を読出し、疑似ランダム信号発生回路を設定することにより、異なる疑似ランダム信号を発生できる。

すなわち、送信側では、第１疑似ランダム信号発生回路の疑似ランダム信号の種類は、暗号鍵設定手段の設定に応じたパラレル・アドレス信号により決まる。このパラレル・アドレス信号は、シ

リアル・アドレス信号に変換されて、送信側から受信側に伝送される。

受信側では、シリアル・アドレス信号をパラレル・アドレス信号に変換して、第２疑似ランダム信号発生回路の疑似ランダム信号を選択する。

よって、送信側及び受信側で、疑似ランダム信号が同じになり、暗号化されたデータを確実に復号化できる。

したがって、送信側の暗号鍵設定手段を変更するのみで、なんら受信側を変更することなく、暗号を変更できる。

［実　施　例］

以下、添付図を参照して、本発明の好適な実施例を説明する。

第１図は、送信側のブロック図である。疑似ランダム信号発生回路は、６段のシフト・レジスタＳＲ１～ＳＲ６の縦続接続段１と、この縦続接続段１の帰還路を選択する切り替え回路２とで構成する。

縦続接続段１のシフト・レジスタのロードＦ及びシフト状態は、制御手段であるマイクロコンピュータ６からの制御信号Ｓ／Ｌが制御する。この制御信号Ｓ／Ｌがロード状態のとき、シフト・レジスタＳＲ１～ＳＲ６は、マイクロコンピュータ６からの初期値データＰ０１～Ｐ０６をロードする。なお、これらシフト・レジスタは、クロック信号ＣＫに同期して動作する。

切り替え回路２は、種々のゲート及び反転器で構成されている。すなわち、アンド・ゲート２１は、シフト・レジスタＳＲ５の出力信号及びマイクロコンピュータ６からの制御信号Ｐ０７を受け、反転器２２は、制御信号Ｐ０７を反転する。アンド・ゲート２３は、シフト・レジスタＳＲ１及び反転器２２の出力を受け、オア・ゲート２４は、アンド・ゲート２１及び２３の出力信号を受ける。よって、制御信号Ｐ０７が高か低かに応じて、シフト・レジスタＳＲ１又はＳＲ５の出力信号がオア・ゲート２４の出力信号となる。

さらに、切り替え回路２では、排他的オア・ゲート２５が、オア・ゲート２４及びシフト・レジスタＳＲ６の出力信号を受け、その排他的オアの結果をシフト・レジスタＳＲ１に帰還している。

よって、シフト・レジスタＳＲ１～ＳＲ６がシフト動作のとき、初期データ及び切り替え回路２の選択に応じた疑似ランダム信号が、シフト・レジスタＳＲ６から発生する。

暗号鍵設定手段５は、接地（低）又は開放（高）を選択する６個のスイッチであり、その設定結果をマイクロコンピュータ６の端子Ｐ１１～Ｐ１６に供給する。

記憶回路であるリード・オンリ・メモリ（ＲＯＭ）３は、縦続接続段１のシフト・レジスタの初期値と、切り替え回路２による帰還路設定データとを複数組記憶している。

マイクロコンピュータ６は、暗号鍵設定手段５の設定に応じてＲＯＭ３をアドレス指定し、対応する初期値及び帰還路設定データを受け、制御信号Ｐ０１～Ｐ０７を発生して、疑似ランダム信号発生回路を設定する。

また、マイクロコンピュータ６は、暗号鍵設定手段５の設定に応じて、端子Ｐ０８～Ｐ１４にパラレル・アドレス信号を発生する。第１変換回路４は、マイクロコンピュータ６からのパラレル・アドレス信号をシリアル・アドレス信号に変換して出力する。

暗号化回路であるスクランブル回路７を、排他的オア・ゲートで構成する。このゲートは、疑似ランダム信号発生回路からの疑似ランダム信号と、データ発生手段（図示せず）からのシリアル・データ（例えば、音声データ）との排他的オアの結果を、暗号文として出力する。

データ／制御信号切り替え回路８は、変換回路４からのシリアル・アドレス信号（ＲＯＭアドレス指定用制御信号）、スクランブル回路７からの暗号文データ（音声データ）、及び同期信号発生回路９からの同期信号を、マイクロコンピュータ６の制御により、クロック信号に同期して切り替え、有線又は無線の通信回線に出力する。この際のタイミング例を第３図に示す。

このようにして、第１図の送信側では、暗号鍵

設定手段5の設定に応じて、データを暗号化し、同期信号及びROMアドレス指定用制御信号と共に、通信回線に出力する。

第2図は、受信側のブロック図である。第1図と同じブロックは、同じ参照番号で示し、異なる部分についてのみ、以下説明する。

データ／制御信号切り替え回路8は、通信回線からの信号を受け、この信号を同期信号検出回路12に供給する。同期信号検出回路12は、第3図に示すように、通信回線からの信号に含まれる同期信号を検出し、この検出結果を第2制御手段であるマイクロコンピュータ6に知らせる。

さらに、データ／制御信号切り替え回路8は、同期信号に応じたマイクロコンピュータ6からの制御信号Po17及びクロック信号に応じて、通信回線からのROMアドレス指定用制御信号（シリアル・アドレス信号）を第2変換回路10に供給すると共に、暗号文データを復号化回路であるデスクランブル回路11に供給する。

第2変換回路10は、シリアル・アドレス信号をパラレル・アドレス信号に変換して、マイクロコンピュータ6の端子Pi8～Pi11に供給する。マイクロコンピュータ6は、このアドレス信号に応じて、ROM3から初期値及び帰還路設定データを読出し、縦続接続段1及び切り替え回路2の第2疑似ランダム信号発生回路を設定する。

受信側のROM3の記憶内容は、送信側のROM3の記憶内容と同じであり、受信側及び送信側の疑似ランダム信号発生回路は、同じ構成なので、受信側は、送信側と同じ疑似ランダム信号を発生する。

デスクランブル回路11は、シフト・レジスタSR6からの疑似ランダム信号、及びデータ／制御信号切り替え回路8からの暗号文データを受ける論理的オア・ゲートである。この構成は、送信側のスクランブル回路7と逆の構成であるので、暗号文データを平文データに変換できる。

上述は、本発明の好適な実施例について説明したが、本発明の精神を逸脱することなく種々の変更ができる。例えば、縦続接続段のシフト・レジスタの段数は、任意の数でもよく、また、帰還路は、任意のシフト・レジスタの出力でもよい。

【発明の効果】

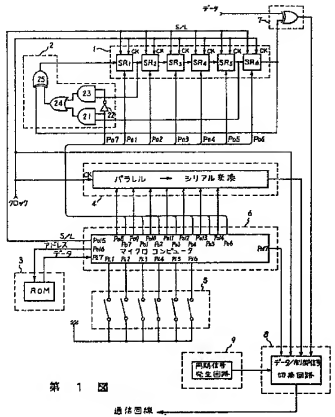
上述の如く、本発明の秘話装置によれば、送信側及び受信側にて、暗号鍵自体を取り替えることなく、容易且つ自由に鍵の設定及び変更が可能である。

4．図面の簡単な説明

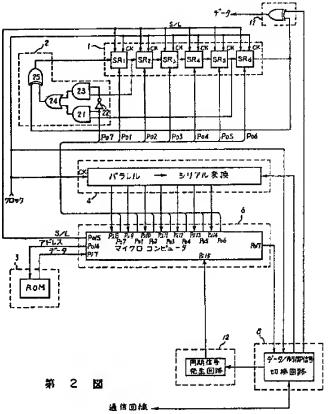
第1図は本発明による送信側のブロック図、第2図は本発明による受信側のブロック図、第3図は本発明による通信区間のタイミング図、第4図は従来の秘話装置のブロック図である。

1，2・・・疑似ランダム信号発生回路
3・・・記憶回路
4，10・・・変換回路
5・・・暗号鍵設定手段
6・・・制御手段
7・・・暗号化回路
8・・・データ／制御信号切り替え回路
11・・・復号化回路

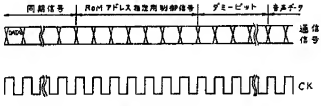
特許出願人　シャープ株式会社
代理人　弁理士　山口邦夫



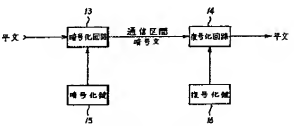
第 1 図



第 2 図



第 3 図



第 4 図

PTO 08-5615

CC = JP
19901005
Kokai
02249333

CONFIDENTIAL CALL DEVICE
[Mitsuwa sochi]

Junji Hirade et al.

UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. JUNE 2008
TRANSLATED BY: THE MCELROY TRANSLATION COMPANY

PUBLICATION COUNTRY	(19):	JP
DOCUMENT NUMBER	(11):	02249333
DOCUMENT KIND	(12):	Kokai
PUBLICATION DATE	(43):	19901005
APPLICATION NUMBER	(21):	170200
APPLICATION DATE	(22):	19890322
INTERNATIONAL CLASSIFICATION[5]	(51):	H 04 L 9/02 9/06 9/14
INVENTORS	(72):	Junji Hirade et al.
APPLICANT	(71):	Sharp Corp.
TITLE	(54):	CONFIDENTIAL CALL DEVICE
FOREIGN TITLE	[54A]:	Mitsuwa sochi

Claim

A type of confidential call device characterized by the following facts:

the sender side has the following parts:

a first pseudo random signal generator using a shift register having a switchable feedback path,

an encoding key setting means that sets the encoding key,

a first storage circuit that stores the initial value and the feedback path setting data of said pseudo random signal generator,

a first control means that reads said initial value and feedback path setting data from said first storage circuit corresponding to said encoding key, and sets said first pseudo random signal generator,

a first converter that converts the parallel address signal to the serial address signal corresponding to said encoding key,

and an encoder that encodes the input data according to the output signal of said first pseudo random signal generator;

and the receiver side has the following parts:

a second pseudo random signal generator that has the same constitution as said first pseudo random signal generator,

a second storage circuit that stores the same contents as said first storage circuit,

a second converter that converts the received serial address signal to a parallel address signal,

a second control means that reads said initial value and feedback path setting data from said second storage circuit according to the parallel address signal from said second converter, and sets said second pseudo random signal generator,

and a decoder that decodes the received data from the output signal of said second pseudo random signal generator.

Detailed explanation of the invention

Industrial application field

The present invention pertains to a type of confidential call device in wired and wireless digital communication.

Prior art

In the wired and wireless communication, when the communication contents are confidential, confidential communication should be performed. For this purpose, on the sender side, the conventional data (plain text) is encoded. The encoded data (encoded text) is used in communication in the wired or wireless communication region. Then, on the receiver side, the encoded text is decoded to the converted text.

Figure 4 is a diagram illustrating a confidential call device in the prior art. In this confidential call device, on the sender side, encoder (13) converts the plain text to the encoded text corresponding to encoding key (means for controlling encoding) (15).

The encoded text from encoder (13) is sent through the wired or wireless communication interval to the receiver side.

On the receiver side, decoder (14) converts the encoded text to the plain text corresponding to decoding key (means for controlling decoding) (16).

Problems to be solved by the invention

In the confidential call device of the prior art shown in Figure 4, the sender side and the receiver side should have the same or independent key(s) for performing encoding and decoding. These keys should

be predetermined corresponding to the encoding, and, each time when the encoding is changed, new keys should be available.

Consequently, one should perform the tedious work in setting and changing the encoding key. In particular, in order to keep the communication confidential, each time, the encoding key should be changed.

Consequently, the purpose of the present invention is to provide a type of confidential call device characterized by the fact that it does not need changing of the encoding key each time when encoding is changed, and it allows easier setting and change of the encoding.

Means to solve the problems

The present invention provides a type of confidential call device characterized by the following facts: the confidential call device of the present invention is divided to the sender side and the receiver side.

The sender side has the following parts:

a first pseudo random signal generator using a shift register having a switchable feedback path,

an encoding key setting means that sets the encoding key,

a first storage circuit that stores the initial value and the feedback path setting data of said pseudo random signal generator,

a first control means that reads said initial value and feedback path setting data from said first storage circuit corresponding to said encoding key, and sets said first pseudo random signal generator,

a first converter that converts the parallel address signal to the serial address signal corresponding to said encoding key,

and an encoder that encodes the input data according to the output signal of said first pseudo random signal generator.

On the other hand, the receiver side has the following parts:

a second pseudo random signal generator that has the same constitution as said first pseudo random signal generator,

a second storage circuit that stores the same contents as said first storage circuit,

a second converter that converts the received serial address signal to a parallel address signal,

a second control means that reads said initial value and feedback path setting data from said second storage circuit according to the parallel address signal from said second converter, and sets said second pseudo random signal generator,

and a decoder that decodes the received data from the output signal of said second pseudo random signal generator.

Operation

The first and second pseudo random signal generators on the sender and receiver sides each use shift registers having a switchable feedback path. Consequently, by changing the feedback path and the initial value, it is possible to generate various driving pseudo random signals.

On the other hand, the first and second storage circuits store the plural phases of the initial value and the feedback path setting data of the pseudo random signal generator. Consequently, corresponding to the setting of the encoding key setting means, the contents of storage of the storage circuit are read, and the pseudo random signal generator is set, so that different pseudo random signals can be generated.

That is, on the sender side, the type of the pseudo random signal of the first pseudo random signal generator depends on the parallel address signal corresponding to setting of the encoding key setting means. This parallel address signal is converted to the serial address signal for transmission from the sender side to the receiver side.

On the receiver side, the serial address signal is converted to the parallel address signal, and the pseudo random signal of the second pseudo random signal generator is selected.

Consequently, on the sender side and receiver side, the pseudo random signals become the same, and the encoded data can be decoded reliably.

As a result, by simply changing the encoding key setting means on the sender side, it is possible to change the encoding without any change on the receiver side.

Application examples

In the following, an explanation will be given regarding a preferable application example of the present invention with reference to the attached figures.

Figure 1 is a block diagram illustrating the sender side. Here, the pseudo random signal generator comprises tandem connected section (1) of 6 sections of shift registers SR1-SR6, and switching circuit (2) that selectively switches the feedback path of said tandem connected section (1).

The load and shift states of the shift registers in tandem connected section (1) are controlled by control signal S/L from microcomputer (6) as the control means. When said control signal S/L is in the load state, shift registers SR1-SR6 load initial value data Po1-Po6 from microcomputer (6). These shift registers work in synchronization to clock signal CK.

Said switching circuit (2) comprises various gates and inverters. That is, ANG gate (21) receives the output signal of shift register SR5 and control signal Po7 from microcomputer (6), and inverter (22) inverts said control signal Po7. AND circuit (23) receives the outputs of shift register SR1 and inverter (22), and OR gate (24) receives the output signals of AND gates (21) and (23). Consequently, corresponding to the high/low level of control signal Po7, the output signal of shift register SR1 or SR5 becomes the output signal of OR gate (24).

In switching circuit (2), exclusive-OR gate (25) receives the output signals of OR gate (24) and shift register SR6, and the result of their exclusive-OR is fed back to shift register SR1.

Consequently, when said shift registers SR1-SR6 perform the shift operation, corresponding to the initial data and selection of switching circuit (2), the pseudo random signal is generated from shift register SR6.

Here, encoding key setting means (5) includes 6 switches for selection of ground (low) or open (high). The setting result is fed to terminals Pi1-Pi6 of microcomputer (6).

Read-only memory (ROM) (3) as the storage circuit stores plural groups of the initial value of the shift register of tandem connected section (1) and the feedback path setting data set by switching circuit (2).

Said microcomputer (6) assigns address for ROM (3) corresponding to setting of encoding key setting means (5). It receives the corresponding initial value and the feedback path setting data, generates control signals Po1-Po7, and sets the pseudo random signal generator.

Also, corresponding to setting of encoding key setting means (5), microcomputer (6) generates the parallel address signal at terminals Po8-Po14. First converter (4) converts the parallel address signal from microcomputer (6) to a serial address signal for output.

As an encoder, scrambler (7) is made of exclusive-OR gate. This gate outputs as encoded text the result of exclusive-OR of the pseudo random signal from the pseudo random signal generator and the serial data (such as voice data) from the data generating means (not shown in the figure).

Under control of microcomputer (6), data/control signal switching circuit (8) switches in synchronization to the clock signal the serial address signal from converter (4) (control signal for assigning ROM address), the encoded text data (voice data) from scrambler (7), and the synchronization

signal from synchronization signal generator (9), and outputs the signals to the wired or wireless communication line. Figure 3 is a diagram illustrating an example of timing in this case.

In this way, on the sender side shown in Figure 1, corresponding to setting of encoding key setting means (5), the data are encoded, and are then output to the communication line together with the synchronization signal and the control signal for assigning the ROM address.

Figure 2 is a block diagram of the receiver side. The same keys as those in Figure 1 are adopted here to indicate the blocks. In the following, an explanation will be given regarding only the different features.

Said data/control signal switching circuit (8) receives the signal from the communication line, and sends the signal to synchronization signal detector (12). As shown in Figure 3, said synchronization signal detector (12) detects the synchronization signal contained in the signal from the communication line, and notifies the detection result to microcomputer (6) as the second control means.

Then, corresponding to control signal Po17 from microcomputer (6) corresponding to the synchronization signal and the clock signal, data/control signal switching circuit (8) sends the control signal for assigning the ROM address from the communication line (serial address signal) to second converter (10), and, at the same time, sends said signal to scrambler (11) as the circuit for decoding the encoded text data.

Second converter (10) converts the serial address signal to the parallel address signal, and sends the signal to terminals Pi8-Pi14 of microcomputer (6). Corresponding to this address signal, microcomputer (6) reads from ROM (3) the initial value and the feedback path setting data, and sets tandem connected section (1) and the second pseudo random signal generator of switching circuit (2).

The storage contents in ROM (3) on the receiver side are the same as those of ROM (3) on the sender side, and the pseudo random signal generators on the sender side and receiver side have the same

constitution. Consequently, the receiver side generates the same pseudo random signal as that on the sender side.

Said scrambler (11) is an exclusive-OR gate that receives the pseudo random signal from shift register SR6 and the encoded text data from data/control signal switching circuit (8). Its constitution is inverted to that of scrambler (7) on the sender side. Consequently, it can convert the encoded text to the plain text data.

In the above, explanation has been made on a preferable application example of the present invention. Various modifications can be made as long as the gist of the present invention is observed. For example, the number of the shift registers of the tandem connected section can be any number. Also, the feedback path may be the output of any shift register.

Effect of the invention

As explained above, according to the confidential call device of the present invention, on the sender side and receiver side, it is possible to perform setting and change of the keys easily and freely without changing the encoding key itself.

Brief description of the figures

Figure 1 is a block diagram illustrating the sender side in the present invention. Figure 2 is a block diagram illustrating the receiver side of the present invention. Figure 3 is a diagram illustrating timing of the communication region in the present invention. Figure 4 is a block diagram illustrating the confidential call device in the prior art.

1, 2 Pseudo random signal generator

3 Storage circuit

4, 10 Converter

5 Encoding key setting means

6 Microcomputer

7 Encoder

8 Data/control signal switching circuit

11 Decoder

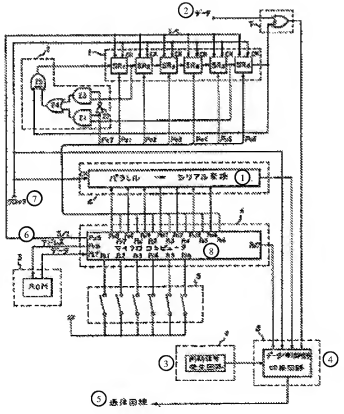


Figure 1

Key: 1 Parallel → serial conversion

2 Data

3 Synchronization signal generator

4 Data/control signal switching circuit

5 Communication line

6 Address data

7 Clock

8 Microcomputer

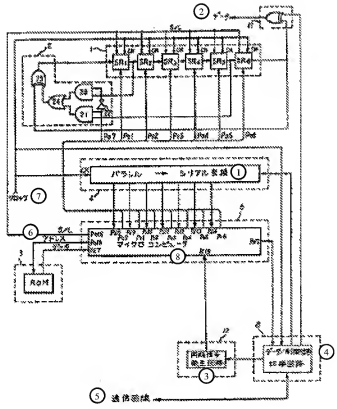


Figure 2

Key: 1 Parallel → serial conversion

2 Data

3 Synchronization signal generator

4 Data/control signal switching circuit

5 Communication line

6 Address data

7 Clock

8 Microcomputer

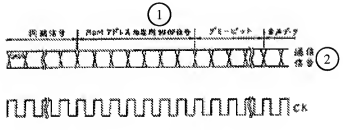


Figure 3

Key: 1 Synchronization signal

Control signal for assigning ROM address

Dummy bits

Voice data

2 Communication signal

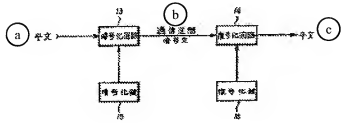


Figure 4

Key: a Plain text

b Communication region

Encoded text

c Plain text

13 Encoder

14 Decoder

15 Encoding key

16 Decoding key